

EXHIBIT 7

Exhibit C

DEFENDANTS' JOINT PROPOSED CLAIM CONSTRUCTIONS AND SUPPORT

Claim Element(s)	Defendants' Construction	Support for Construction
		<p data-bbox="272 888 297 1003">* * *</p> <p data-bbox="345 163 597 1098">Johnson does not teach or suggest a session identifier but rather teaches a credentials identifier. A credentials identifier is a "small value" used to access a "credentials structure" which is maintained on the server. See Johnson, column 5, lines 54-65. Each time a request is made, the server reconstructs "an image of the user." Johnson, column 5, lines 40-42. Johnson uses the credentials identifier to locate the credentials structure from which the image of the user is reconstructed.</p> <p data-bbox="646 195 751 1098">Applicants' invention, on the other hand, does not need to perform this reconstruction, because the session identifier itself contains sufficient information to validate that the request is authorized.</p> <p data-bbox="784 1014 808 1098">*****</p> <p data-bbox="857 174 1182 1098">For example, Freeman-Benson teaches a "specialized URL" containing an access key which is simply an encrypted login name and password. Furthermore, Freeman-Benson teaches storing the specialized URL, that is, the request (the normal URL) along with the access key. Thus, later use of this stored specialized URL will result in a repetition of the original request, without requiring further authorization. Freeman-Benson does not append the specialized URL to subsequent requests - doing so would result in a meaningless request: one URL appended by another URL.</p> <p data-bbox="1230 174 1409 1098">Applicants' invention, on the other hand, stores the SID and appends the stored SID to each URL or request to the particular server that provided the SID, thus defining a session. That is, subsequent requests to the server from the browser do not require the user to enter additional verification information, even for different requests, because the SID</p>

Claim Element(s)	Defendants' Construction	Support for Construction
		<p>both commercially and academically. Most of them use "hot spots" in documents, like icons, or highlighted phrases, as sensitive areas, touching a hot spot with a mouse brings up the relevant information, or expands the text on the screen to include it. Imagine, then, the references in this document, all being associated with the network address of the thing to which they referred, so that while reading this document you could skip to them with a click of the mouse.</p> <p>"Hypertext" is a term coined in the 1950s by Ted Nelson [...], which has become popular for these systems, although it is used to embrace two different ideas. One idea (which is relevant to this problem) is the concept: "Hypertext": Human- readable information linked together in an unconstrained way.</p> <p>The other idea, which is independent and largely a question of technology and time, is of multimedia documents which include graphics, speech and video. I will not discuss this latter aspect further here, although I will use the word "Hypermedia" to indicate that one is not bound to text." Information Management: A Proposal, <i>see</i> CNZ0021631.</p> <p>"2 / Concepts of Hypertext and Hypermedia</p> <p>Hypertext and Hypermedia- Definition and History</p> <p>What does this rainy-night tale have to do with hypertext and hypermedia? Everything. The essential distinction of both hypertext and hypermedia is the automation of the linking process that Nancy and I went through, first to find General Buford and then to investigate the other points that interested us.</p>

Claim Element(s)	Defendants' Construction	Support for Construction
service request to which has been appended by the client, wherein communications between the client and server system are according to hypertext transfer protocol;	formats common to the Web on or before June 7, 1995.	<p>requires a special browser which can handle such communications and was generally not suitable for early browser formats common to the Web. However, it may now be implemented in cookie compatible browsers." 4:23-29 (emphasis added.)</p> <p>"[i]n another embodiment, a server access control may be maintained by programming the client browser to store an SID or a similar tag for use in each URL call to that particular server. This embodiment, however, requires a special browser which can handle such communications and is generally not suitable for the standard browser format common to the Web." US 5,708,780 at 4:25-31 (emphasis added.)</p> <p>"Applicants' invention uses a "session identifier" or SID to provide a "session" of communications between a client system and a server system in a "stateless" session environment. An SID containing enough information to support a session is appended to the initial and subsequent requests. This information can include, for example, an authorization identifier, a user identifier, an accessible domain, a key identifier, an expiration time, a date, the address of the user computer, and/or an unforgeable digital signature "such as a cryptographic hash of all of the other items in the SID encrypted with a secret key." Specification as filed, page 6, lines 16-21. The present invention is particularly suited to restricting access to server sites on the World Wide Web.</p> <p>A user's user name and password is verified once, at the beginning of a session, and a SID is created upon verification.</p> <p style="text-align: center;">* * *</p> <p>Upon receiving the SID from the server system, the client browser stores</p>

Claim Element(s)	Defendants' Construction	Support for Construction
		<p>in response to the request, and returns to the client a credentials identifier associated with the newly created credentials record. When the client presents the credentials identifier in subsequent requests, the server uses the credentials identifier to retrieve the credentials record, and from the credentials record validates the request. Access rights are stored on the server itself, in the credentials record, and are not included in the credentials identifier. See, for example, Johnson, column 5, lines 50-65.</p> <p>* * *</p> <p>For example, Freeman-Benson teaches a "specialized URL" containing an access key which is simply an encrypted login name and password. Furthermore, Freeman-Benson teaches storing the specialized URL, that is, the request (the normal URL) along with the access key. Thus, later use of this stored specialized URL will result in a repetition of the original request, without requiring further authorization. Freeman-Benson does not append the specialized URL to subsequent requests - doing so would result in a meaningless request: one URL appended by another URL.</p> <p>Applicants' invention, on the other hand, stores the SID and appends the stored SID to each URL or request to the particular server that provided the SID, thus defining a session. That is, subsequent requests to the server from the browser do not require the user to enter additional verification information, even for different requests, because the SID which accompanies each request provides validation.</p> <p>In addition, Freeman-Benson, at the time of its publication, worked with "all existing WWW browsers." Freeman-Benson, paragraph 26, page 5, original emphasis. Such browsers as existed at that time would not support Applicants' claimed invention, which, as of the priority date, required a modified browser. See Specification as filed, page 8, lines 15-</p>

3/20/2009
Page 99 of 110

Claim Element(s)	Defendants' Construction	Support for Construction
		<p>19. Of course, "modern" browsers which support cookies are such "modified" browsers." Amendments and Remarks with Request for Continued Examination – December 28, 2001 (emphasis added.)</p> <p>“With this response Applicants supplement their evidence of reduction to practice prior to the effective date of the Kahan reference. The present application is a continuation of U.S. Patent application, serial number 08/474,096 which subsequently issued as U.S. patent number 5,708,780 (the '780 patent). The entire teaching of the parent specification was incorporated by reference into the continuation application. The specification of the '780 patent includes computer code embodying the invention.</p> <p style="text-align: center;">* * *</p> <p>Later, on the page that spans columns 53-54 the TICKET_INTERLOCALSID function performs the step of appending the stored session identifier to each subsequent distinct request from the client to the server.” Response To Office Action, August 31, 2004 (emphasis added.)</p> <p>“Schedule 1 describes ‘the client storing the session identifier for use in subsequent distinct requests to the server system,’ such as on page 5 of Schedule 1 (emphasis added):</p>

Claim Element(s)	Defendants' Construction	Support for Construction
		<p>SID, the Internet server subjects the client to an authorization routine prior to issuing the SID, the SID being protected from forgery. A content server initiates the authorization routine by redirecting the client's request to an authentication server which may be at a different host. Upon receiving a redirected request, the authentication server returns a response to interrogate the client and then issues an SID to a qualified client. For a new client, the authentication server may open a new account and issue an SID thereafter. A valid SID typically comprises a user identifier, an accessible domain, a key identifier, an expiration time such as date, the IP address of the user computer, and an unforgeable digital signature such as a cryptographic hash of all of the other items in the SID encrypted with a secret key. The authentication server then forwards a new request consisting of the original URL appended by the SID to the client in a REDIRECT. The modified request formed by a new URL is automatically forwarded by the client browser to the content server.” 3: 6-41 (emphasis added)</p> <p>“FIG. 2A is a flowchart detailing the preferred process of the present invention and FIG. 4 illustrates a sample Web page displayed at a client by a browser. The page includes text 404 which includes underlined link text 412. The title bar 408 and URL bar 402 display the title and URL of the current web page, respectively. As shown in FIG. 4, the title of the page is "Content Home Page" and the corresponding URL is "http://content.com/homepage". When a cursor 414 is positioned over link text 412b, the page which would be retrieved by clicking a mouse is typically identified in a status bar 406 which shows the URL for that link. In this example the status bar 406 shows that the URL for the pointed link 412b is directed to a page called "advertisement" in a commercial content server called "content". By clicking on the link text, the user causes the browser to generate a URL GET request at 100 in FIG. 2A. The browser forwards the request to a content server 120,</p>

3/20/2009
Page 109 of 110

Claim Element(s)	Defendants' Construction	Support for Construction
		<p>which processes the request by first determining whether the requested page is a controlled document 102. If the request is directed to an uncontrolled page, as in "advertisement" page in this example, the content server records the URL and the IP address, to the extent it is available, in the transaction log 114. The content server then sends the requested page to the browser 116 for display on the user computer 117.</p> <p>If the request is directed to a controlled page, the content server determines whether the URL contains an SID 102. For example, a URL may be directed to a controlled page name "report", such as "http://content.com/report", that requires an SID. If no SID is present, as in this example, the content server sends a "REDIRECT" response 122 to the browser 100 to redirect the user's initial request to an authentication server 200 to obtain a valid SID. The details of the authentication process are described in FIG. 2B and will be discussed later, but the result of the process is an SID provided from the authentication server to the client. In the above example, a modified URL appended with an SID may be:</p> <p>"http://content.com/[SID]/report". The preferred SID is a sixteen character ASCII string that encodes 96 bits of SID data, 6 bits per character. It contains a 32-bit digital signature, a 16-bit expiration date with a granularity of one hour, a 2-bit key identifier used for key management, an 8-bit domain comprising a set of information files to which the current SID authorizes access, and a 22-bit user identifier. The remaining bits are reserved for expansion. The digital signature is a cryptographic hash of the remaining items in the SID and the authorized IP address which are encrypted with a secret key which is shared by the authentication and content servers. If the initial GET URL contains a SID, the content server determines whether the request is directed to a page within the current domain 106. If the request having a SID is</p>

Claim Element(s)	Defendants' Construction	Support for Construction
		<p>directed to a controlled page of a different domain, the SID is no longer valid and, again, the user is redirected to the authentication server 122. If the request is for a controlled page within the current domain, the content server proceeds to log the request URL, tagged with SID, and the user IP address in the transaction log 108. The content server then validates the SID 110." 5: 18-6:8 (emphasis added.)</p> <p>'639 Patent, FIGS 2A-3.</p>